Sophos Enterprise Console 5.2

Guia:

Manual de instalação do Sophos Enterprise Console 5.2

Data do Documento: Abril de 2013

Conteúdo

1. Sobre este manual 3
2. Requisitos de Instalação 4
3. Ambientes com Policy Editor 5
4. Instalando o Sophos Enterprise Console 6
5. Configurações recomendadas 19
   - 5.1. Anti-virus and HIPS 19
   - 5.2. Firewall 22
   - 5.3. Tamper protection 23
   - 5.4. Patch 24
6. Instalando os endpoints (deploy) 25

1. Sobre este manual

Este manual descreve os procedimentos necessários para realizar a instalação do Sophos Enterprise Console 5.2.

Com o Sophos Enterprise Console, é possível gerenciar todos os computadores protegidos pelo Sophos Endpoint, possibilitando inclusive o gerenciamento de diferentes sistemas operacionais e versões usando apenas uma interface.

2. Requisitos de Instalação

1.1. Requisitos para instalar o Sophos Enterprise Console: http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/management-console/system-requirements.aspx

1.2. Requisitos para instalar o Sophos Antivírus nos computadores da rede:

1.2.1. Windows: http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/windows/system-requirements.aspx

1.2.2. Linux: http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/linux/system-requirements.aspx

1.2.3. Mac OS X: http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/mac/system-requirements.aspx

1.2.4. NetApp: http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/netapp/system-requirements.aspx

1.2.5. UNIX: http://www.sophos.com/en-us/products/endpoint/endpoint-security-and-data-protection/components/anti-virus-protection/unix/system-requirements.aspx

3. Ambientes com Policy Editor

Em ambientes que já possuem o “Sophos SafeGuard Policy Editor” será necessário:

- Fazer backup do banco de dados e certificados do Policy Editor.
- Desinstalar o Policy Editor caso o mesmo esteja instalado no mesmo computador que o servidor do Sophos.

Pelo “Adicionar ou remover programas”, verifique se o “Sophos SafeGuard <versão> Policy Editor” está instalado, caso seu ambiente não possua o Policy Editor, pule para o item 4.

Gerando backup:

3.1. Abra o Policy Editor (Iniciar > Todos os programas > Sophos > SafeGuard).
3.2. Clique no menubar “Tools” e clique em “Options”.
3.3. Na guia “Certificates”, em “Company Certificate”, clique no botão “Export”.
3.4. Informe a senha “!s0ph0sSDE!” (sem aspas) e clique em “OK” (esta senha será usada apenas para importar o arquivo novamente durante a instalação).
3.5. Altere o nome do arquivo para “Company.p12” (salve o arquivo na pasta “C:\Sophos_Backup”) e clique em “Salvar”.
3.6. Em “Certificate of ‘Administrator’”, clique no botão “Export”.
3.7. Informe a senha “!s0ph0sSDE!” (sem aspas) e clique em “OK” (esta senha será usada apenas para importar o arquivo novamente durante a instalação).
3.8. Altere o nome do arquivo para “Officer.p12” (salve o arquivo na pasta “C:\Sophos_Backup”) e clique em “Salvar”.
3.9. Clique na guia “Database backup/restore” e clique no botão “Backup database”.
3.10. Clique no botão “Sim” para gerar um backup novo e clique no botão “OK” quando o backup finalizar.
3.11. Logo acima do botão “Backup database”, está informado o caminho onde o backup foi gerado, mova este arquivo para a pasta “C:\Sophos_Backup”.
3.12. Na janela “Options”, clique em “OK” e feche a janela do Policy Editor.

Desinstalado o Policy Editor:

Apenas desinstale o Policy Editor caso ele esteja instalado no mesmo computador que o servidor do Sophos.

Para isto, no “Adicionar ou remover programas”, selecione o item “Sophos SafeGuard <versão> Policy Editor” e clique no botão “Remover”. No termino da remoção, será solicitado a reinicialização do servidor.

4. Instalando o Sophos Enterprise Console

4.1. Faça download e execute o arquivo “sec_52_sfx.exe”, link para download: http://downloads.m3corp.com.br/sophos10/sec_52_sfx.exe

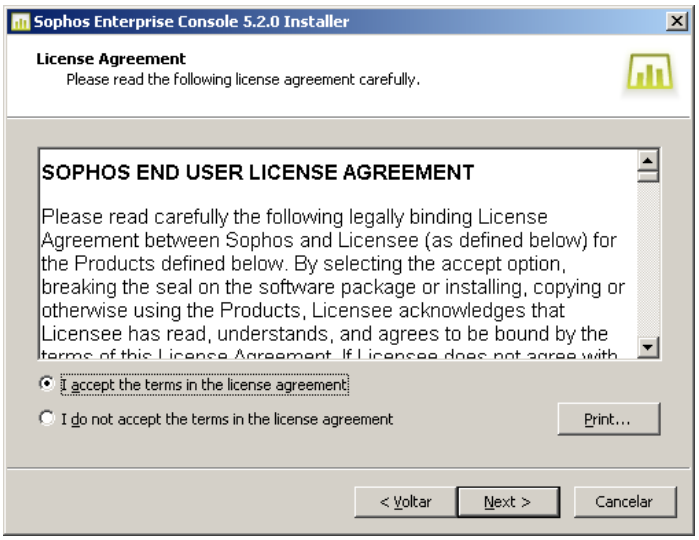
4.2. Clique no botão “Install”.

4.3. Aguarde enquanto os arquivos de instalação são extraídos.

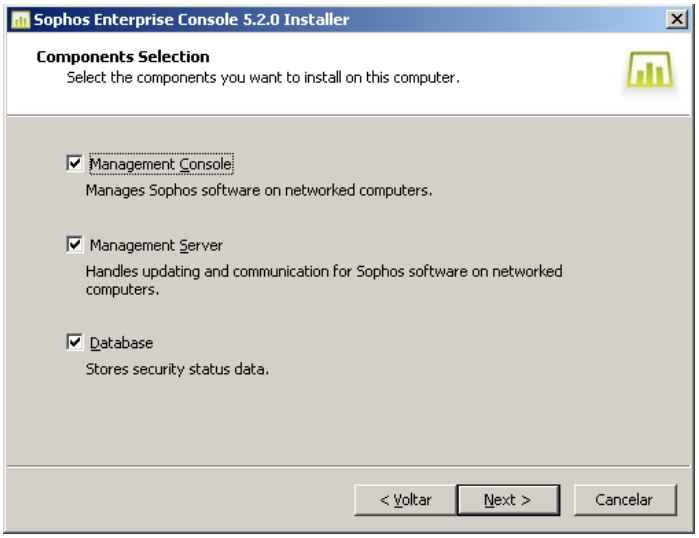
4.4. Clique no botão “Avançar”.

Sophos Enterprise Console 5.2.0 Installer
SOPHOS
Welcome to the Sophos Enterprise Console 5.2.0 Installer
The program will install Sophos Enterprise Console 5.2.0 on your computer.
To continue, click Next.
WARNING: This program is protected by copyright laws and international treaties.
< Voltar
Next >
Cancelar

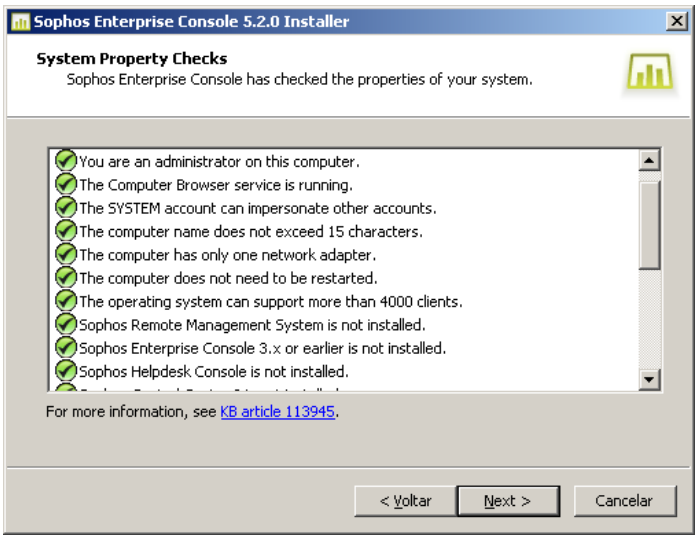
4.5. Clique em “I accept the terms in the license agreement” e clique no botão “Avançar”.


Sophos Enterprise Console 5.2.0 Installer
License Agreement
Please read the following license agreement carefully.
SOPHOS END USER LICENSE AGREEMENT
Please read carefully the following legally binding License Agreement between Sophos and Licensee (as defined below) for the Products defined below. By selecting the accept option, breaking the seal on the software package or installing, copying or otherwise using the Products, Licensee acknowledges that Licensee has read, understands, and agrees to be bound by the
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print...
< Voltar
Next >
Cancelar

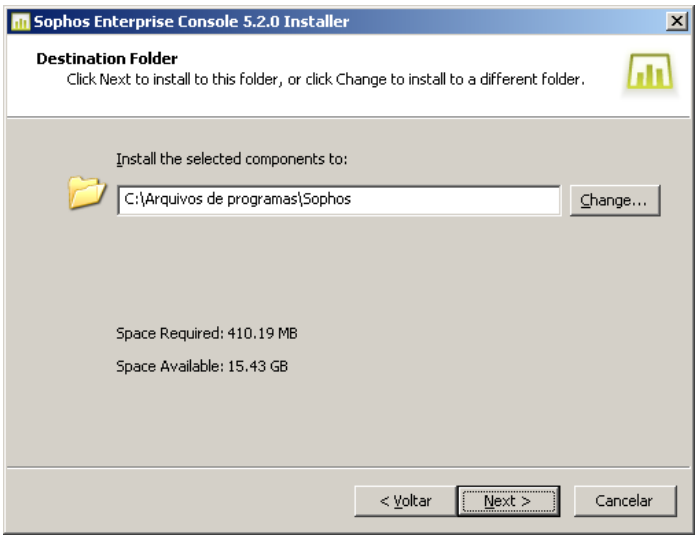
4.6. Verifique se as três opções estão selecionadas e clique em “Avançar”.


Sophos Enterprise Console 5.2.0 Installer
Components Selection
Select the components you want to install on this computer.
Management Console
Manages Sophos software on networked computers.
Management Server
Handles updating and communication for Sophos software on networked computers.
Database
Stores security status data.
< Voltar
Next >
Cancelar

4.7. Caso algum item crítico for detectado, o item será sinalizado com o símbolo , itens críticos devem ser corrigidos antes de prosseguir com a instalação. Em caso de dúvida sobre algum item listado, verifique o artigo 113945 da Sophos (http://www.sophos.com/support/knowledgebase/article/113945.html)


Sophos Enterprise Console 5.2.0 Installer
System Property Checks
Sophos Enterprise Console has checked the properties of your system.
You are an administrator on this computer.
The Computer Browser service is running.
The SYSTEM account can impersonate other accounts.
The computer name does not exceed 15 characters.
The computer has only one network adapter.
The computer does not need to be restarted.
The operating system can support more than 4000 clients.
Sophos Remote Management System is not installed.
Sophos Enterprise Console 3.x or earlier is not installed.
Sophos Helpdesk Console is not installed.
For more information, see KB article 113945.
< Voltar
Next >
Cancelar

4.8. Na tela “Destination Folder”, clique no botão “Avançar”.


Sophos Enterprise Console 5.2.0 Installer
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install the selected components to:
C:\Arquivos de programas\Sophos
Change...
Space Required: 410.19 MB
Space Available: 15.43 GB
< Voltar
Next >
Cancelar

4.9. Na tela “Database Details”, selecione a opção “Create a new instance called ‘SOPHOS’”.

4.10. Clique no botão “Browse”.

4.11. Caso o computador esteja em um domínio no entanto o computador **não** é o “domain controller” (servidor do Active Directory):

4.11.1. Clique no botão “Locais”.

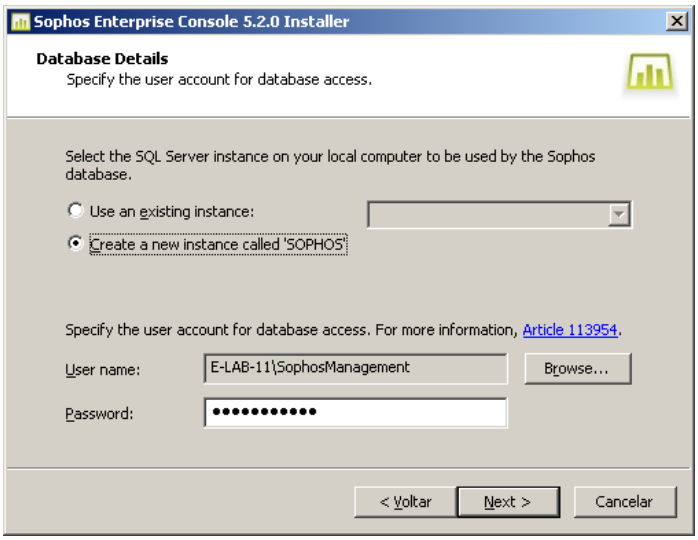
4.11.2. Selecione o nome do computador onde a instalação está sendo executado.

4.11.3. Clique no botão “OK”.

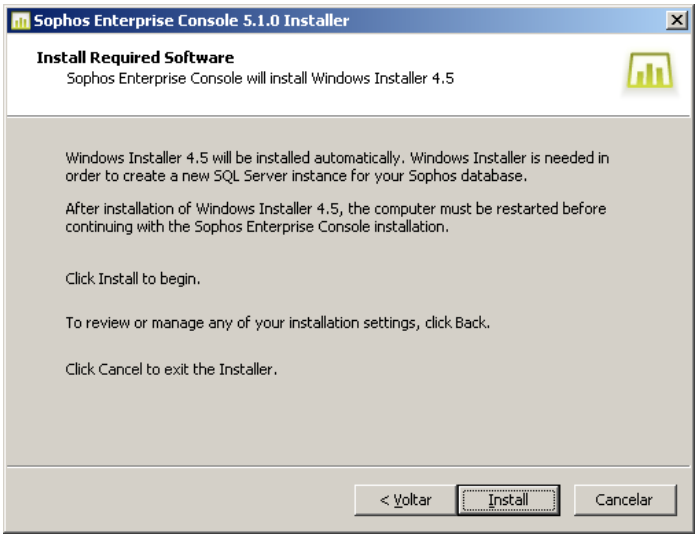
4.12. Informe o usuário “SophosManagement” e clique no botão “OK”.

4.13. Em “Password”, informe: **!s0ph0sMGR!**

4.14. Clique no botão “Avançar”.


Sophos Enterprise Console 5.2.0 Installer
Database Details
Specify the user account for database access.
Select the SQL Server instance on your local computer to be used by the Sophos database.
Use an existing instance:
Create a new instance called 'SOPHOS'
Specify the user account for database access. For more information, Article 113954.
User name:
E-LAB-11\SophosManagement
Browse...
Password:
< Voltar
Next >
Cancelar

4.15. Caso o “Windows Installer 4.5” não esteja instalado, o wizard de instalação irá realizar a instalação do mesmo. Neste caso clique no botão “Install”.

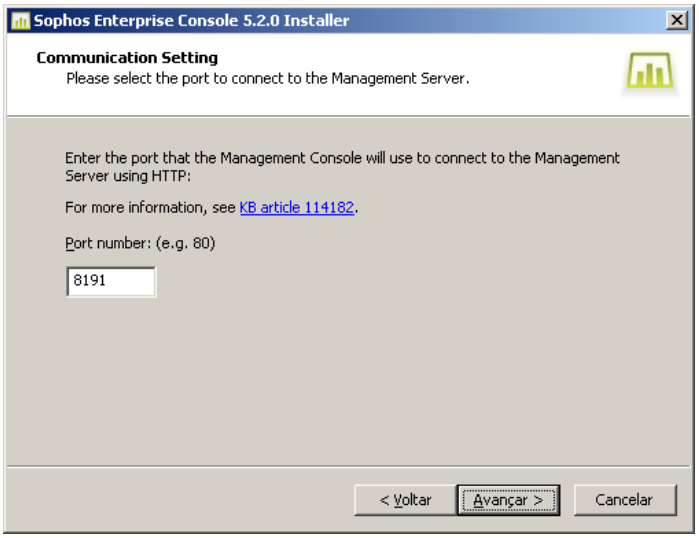

Sophos Enterprise Console 5.1.0 Installer
Install Required Software
Sophos Enterprise Console will install Windows Installer 4.5
Windows Installer 4.5 will be installed automatically. Windows Installer is needed in order to create a new SQL Server instance for your Sophos database.
After installation of Windows Installer 4.5, the computer must be restarted before continuing with the Sophos Enterprise Console installation.
Click Install to begin.
To review or manage any of your installation settings, click Back.
Click Cancel to exit the Installer.
< Voltar
Install
Cancelar

4.16. Caso o “Windows Installer 4.5” foi instalado, será solicitado a reinicialização do computador, clique em “Concluir” para reiniciar o computador. Caso não queira reiniciar o computador neste momento, desmarque a opção “Restart now” e clique em “Concluir”. Após reiniciar, volte para o passo 4.4.

OBS: Após reiniciar o computador, o instalador será executado automaticamente, caso o mesmo usuário seja usado no logon. Caso seja necessário executar o instalador manualmente, execute o arquivo “C:\sec_52\ServerInstaller\Setup.exe”.

Sophos Enterprise Console 5.2.0 Installer
SOPHOS
Installation of Enterprise Console is ready to resume
Windows Installer 4.5 has been successfully installed.
To continue installing Sophos Enterprise Console 5.2.0 you must restart the computer. The Enterprise Console installer will start again automatically.
To restart now, click Finish. To restart later clear the box below and click Finish.
Restart now
< Voltar
Concluir
Cancelar

4.17. Na tela “Communication Setting”, altere a porta para “8191” e clique no botão “Avançar”.


Sophos Enterprise Console 5.2.0 Installer
Communication Setting
Please select the port to connect to the Management Server.
Enter the port that the Management Console will use to connect to the Management Server using HTTP:
For more information, see KB article 114182.
Port number: (e.g. 80)
8191
< Voltar
Avançar >
Cancelar

4.18. Na tela “Sophos Update Manager Credentials”, clique no botão “Browse”.

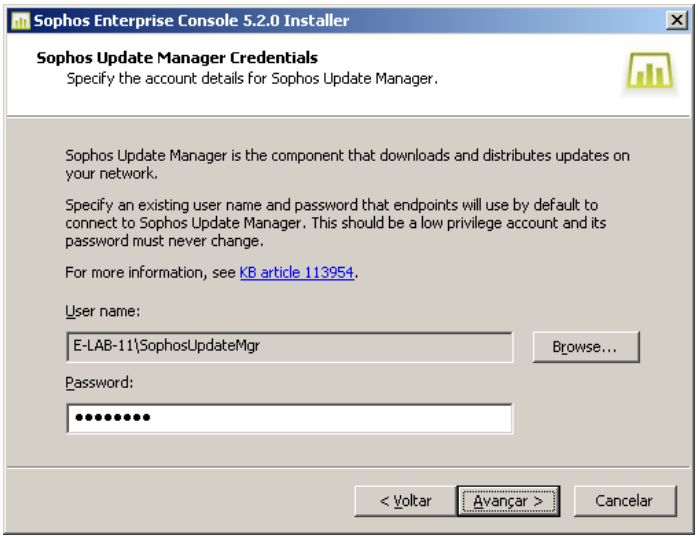
4.19. Caso o computador esteja em um domínio, no entanto o computador não é o “domain controller” (servidor do Active Directory):

4.19.1. Clique no botão “Locais”.

4.19.2. Selecione o nome do computador onde a instalação está sendo executado.

4.19.3. Clique no botão “OK”.

4.20. Informe o usuário “SophosUpdateMgr” e clique no botão “OK”.
4.21. Em “Password”, informe: **!s0ph0s!**
4.22. Clique em “Avançar”.

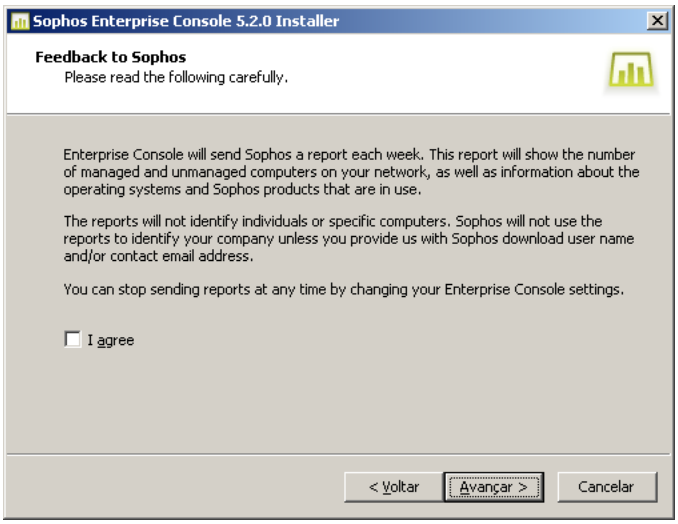

Sophos Enterprise Console 5.2.0 Installer
Sophos Update Manager Credentials
Specify the account details for Sophos Update Manager.
Sophos Update Manager is the component that downloads and distributes updates on your network.
Specify an existing user name and password that endpoints will use by default to connect to Sophos Update Manager. This should be a low privilege account and its password must never change.
For more information, see KB article 113954.
User name:
E-LAB-11\SophosUpdateMgr
Browse...
Password:
< Voltar
Avançar >
Cancelar

4.23. Na tela “Manage Encryption”, caso você **não queira** usar a criptografia do Sophos (full disk encryption), marque a opção “Do not manage encryption” e clique em “Avançar” (é possível alterar isto após a instalação). Pule para o passo 4.25.
4.24. Caso você queira usar a criptografia do Sophos (full disk encryption):

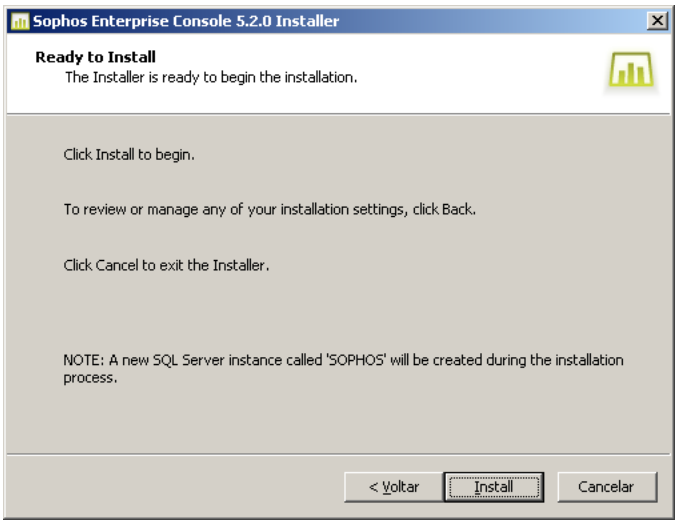
4.24.1. Selecione a opção “Manage encryption” e clique no botão “Avançar”.
4.24.2. Caso você ainda não possui a criptografia da Sophos, pule para o passo 4.24.7.
4.24.3. Caso você possui os backups dos certificados, marque a opção “Existing installation” e clique no botão “Avançar”.
4.24.4. Em “master security officer”, importe o arquivo “Officer.p12” e informe a senha “!s0ph0sSDE!” (ou outra senha usada ao gerar o backup).
4.24.5. Em “company certificate”, importe o arquivo “Company.p12” e informe a senha “!s0ph0sSDE!” (ou outra senha usada ao gerar o backup).
4.24.6. Clique no botão “Avançar” e pule para o passo 4.25.
4.24.7. Selecione a opção “New instalation” e clique no botão “Avançar”.
4.24.8. Na tela “Back up Certificates”, informe a senha “!s0ph0sSDE!” (sem aspas) e altere o caminho do backup para um local seguro. Clique no botão “Avançar”.

OBS: Salve os certificados em um local seguro bem como a senha usada. Caso ocorrer algum problema no servidor (exemplo: o HD do servidor foi corrompido, o servidor foi formatado, etc), será necessário deste certificado para restaurar o servidor.
Em casos onde o servidor foi perdido, sem este certificado, não será possível recuperar o servidor para voltar a gerenciar o software de criptografia instalado nos computadore, bem como realizar métodos de recuperação.
Os seguintes arquivos de backup são gerados durante o a instalação:
company.cer, company.p12, mso.cer e mso.p12.

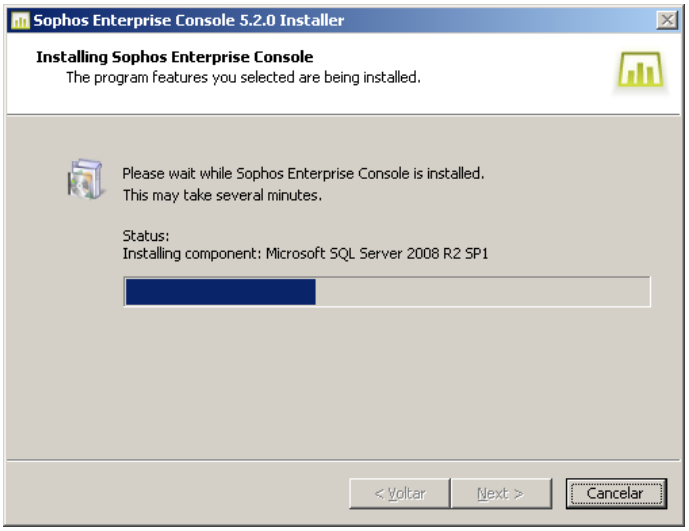
4.25. Na tela “Feedback to Sophos”, desmarque a opção “I agree” e clique em “Avançar”.


Sophos Enterprise Console 5.2.0 Installer
Feedback to Sophos
Please read the following carefully.
Enterprise Console will send Sophos a report each week. This report will show the number of managed and unmanaged computers on your network, as well as information about the operating systems and Sophos products that are in use.
The reports will not identify individuals or specific computers. Sophos will not use the reports to identify your company unless you provide us with Sophos download user name and/or contact email address.
You can stop sending reports at any time by changing your Enterprise Console settings.
I agree
< Voltar
Avançar >
Cancelar

4.26. Na tela “Ready to Install”, clique no botão “Install” para iniciar a instalação.


Sophos Enterprise Console 5.2.0 Installer
Ready to Install
The Installer is ready to begin the installation.
Click Install to begin.
To review or manage any of your installation settings, click Back.
Click Cancel to exit the Installer.
NOTE: A new SQL Server instance called 'SOPHOS' will be created during the installation process.
< Voltar
Install
Cancelar

4.27. Aguarde a instalação finalizar.


Sophos Enterprise Console 5.2.0 Installer
Installing Sophos Enterprise Console
The program features you selected are being installed.
Please wait while Sophos Enterprise Console is installed.
This may take several minutes.
Status:
Installing component: Microsoft SQL Server 2008 R2 SP1
< Voltar
Next >
Cancelar

4.28. Após finalizar a instalação, será solicitado um logoff, clique no botão “Concluir”, o logoff será realizado (em alguns casos pode se solicitado a reinicialização).

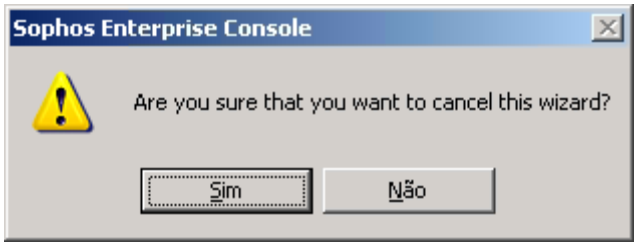
Sophos Enterprise Console 5.2.0 Installer
SOPHOS
Installation of Sophos Enterprise Console 5.1.0 is complete
Sophos Enterprise Console 5.1.0 has been successfully installed.
To ensure Sophos Enterprise Console runs correctly, you need to log off.
To log off now, click Finish. To log off later clear the box below and click Finish.
Log off now
< Voltar
Concluir
Cancelar

4.29. Faça login no servidor, após isto o Sophos Enterprise Console irá iniciar automaticamente.

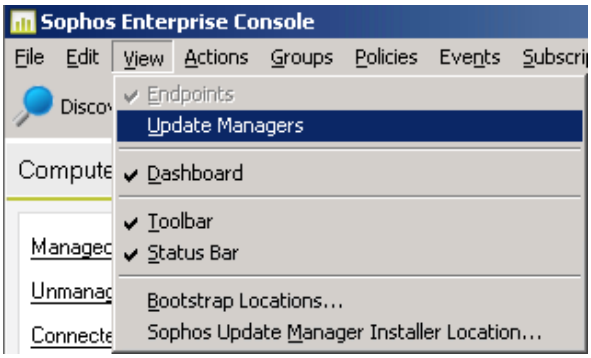
4.30. Na tela “Download Security Software Wizard”, clique no botão “Cancelar”.

Download Security Software Wizard
SOPHOS
Welcome to the Download Security Software Wizard
This wizard will guide you through the process of downloading and automatically updating the security software you need. You will need the username and password supplied to you by Sophos.
To continue, click "Next".
< Voltar
Avançar >
Cancelar

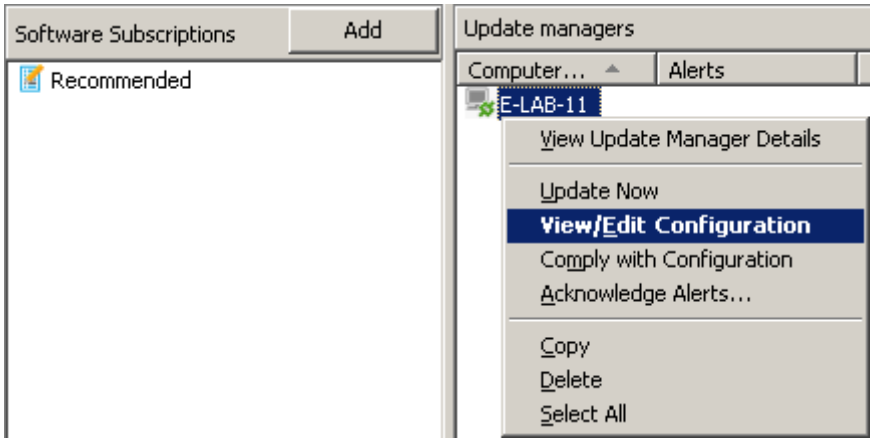
4.31. Na tela de confirmação, clique em “Sim”.



4.32. No menu bar, clique em “View” > “Update Managers (caso esta opção estiver desabilitada, pule para o próximo passo).”



4.33. Clique com o Botão direito no servidor e clique em “View/Edit Configuration”.



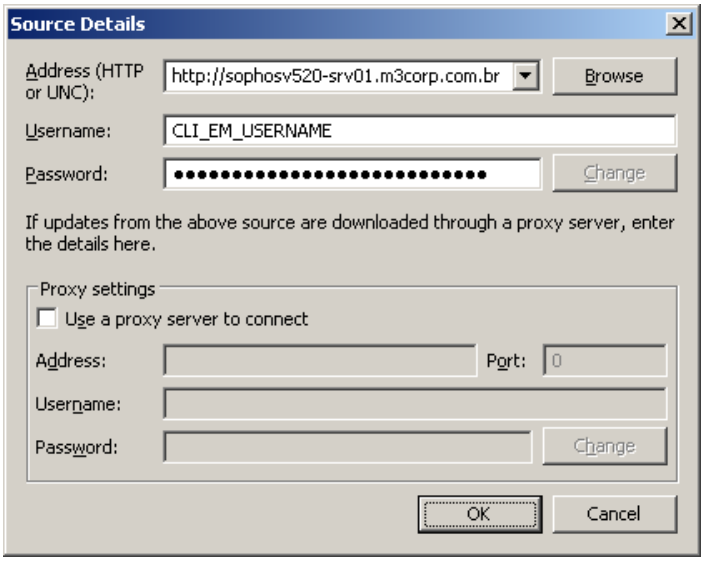
4.34. Clique no botão “Add”.

4.35. Em “Address”, informe: http://sophosv520-srv01.m3corp.com.br

4.36. Em “Username”, informe seu usuário de atualização (informado em sua licença).

4.37. Em “Password”, informe a senha do seu usuário de atualização.

4.38. Clique no botão “OK”.



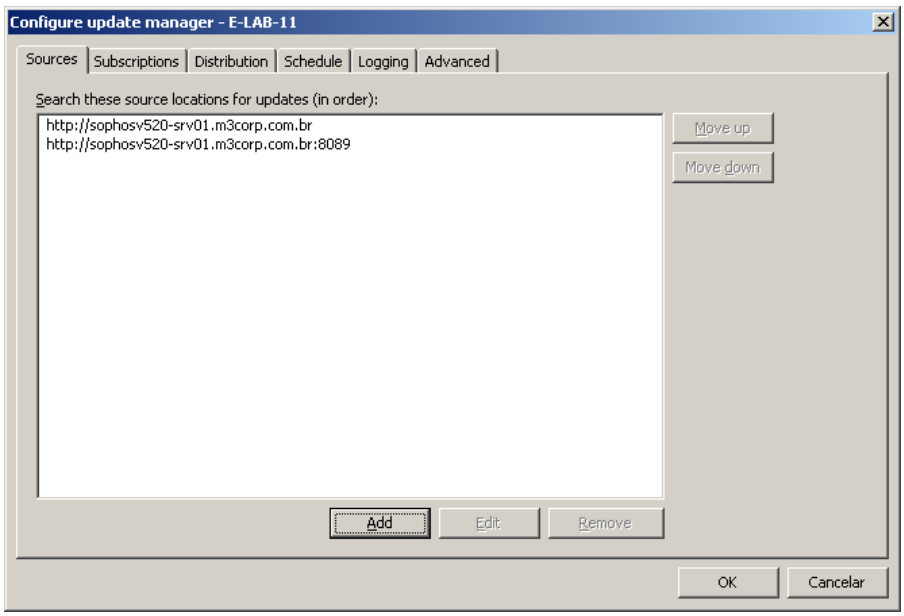
4.39. Clique novamente no botão “Add”.

4.40. Em “Address”, informe: http://sophosv520-srv01.m3corp.com.br:8089

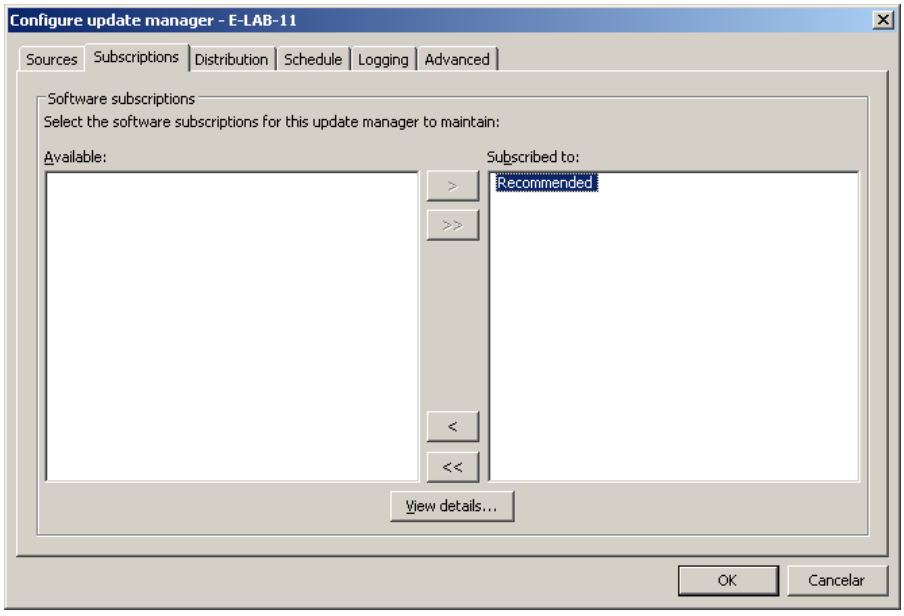
4.41. Em “Username”, informe seu usuário de atualização (informado em sua licença).

4.42. Em “Password”, informe a senha do seu usuário de atualização.

4.43. Clique no botão “OK” para salvar a nova “Source”.

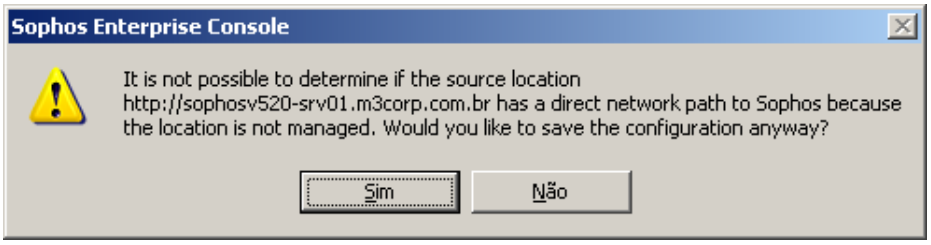


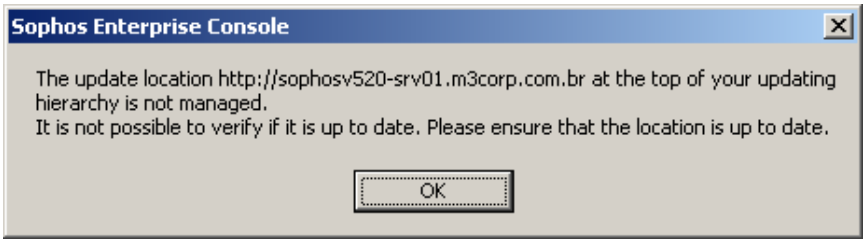
4.44. Clique na guia/aba “Subscription”, selecione o item “Recommended”, clique no botão “>” e então clique no botão “OK”.



4.45. Na janela “Configure update manager”, clique no botão “OK”.

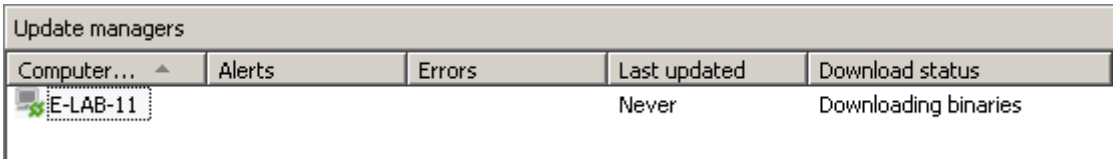
4.46. Duas mensagens serão exibidas (conforme os exemplos das imagens abaixo), clique no botão “Sim” e em seguida clique no botão “OK”:


Sophos Enterprise Console
It is not possible to determine if the source location http://sophosv520-srv01.m3corp.com.br has a direct network path to Sophos because the location is not managed. Would you like to save the configuration anyway?
Sim
Não

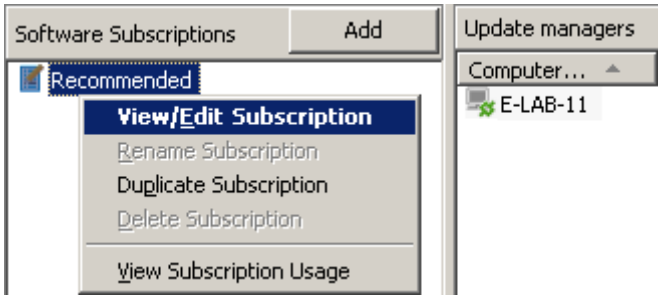

Sophos Enterprise Console
The update location http://sophosv520-srv01.m3corp.com.br at the top of your updating hierarchy is not managed.
It is not possible to verify if it is up to date. Please ensure that the location is up to date.
OK

4.47. Clique com o botão direito no servidor e clique em “Update now”.

4.48. Aguarde a coluna “Download status” alterar de “Downloading binaries” para “Last checked at: <data atual>” (isto pode demorar em torno de 1 a 2 minutos).

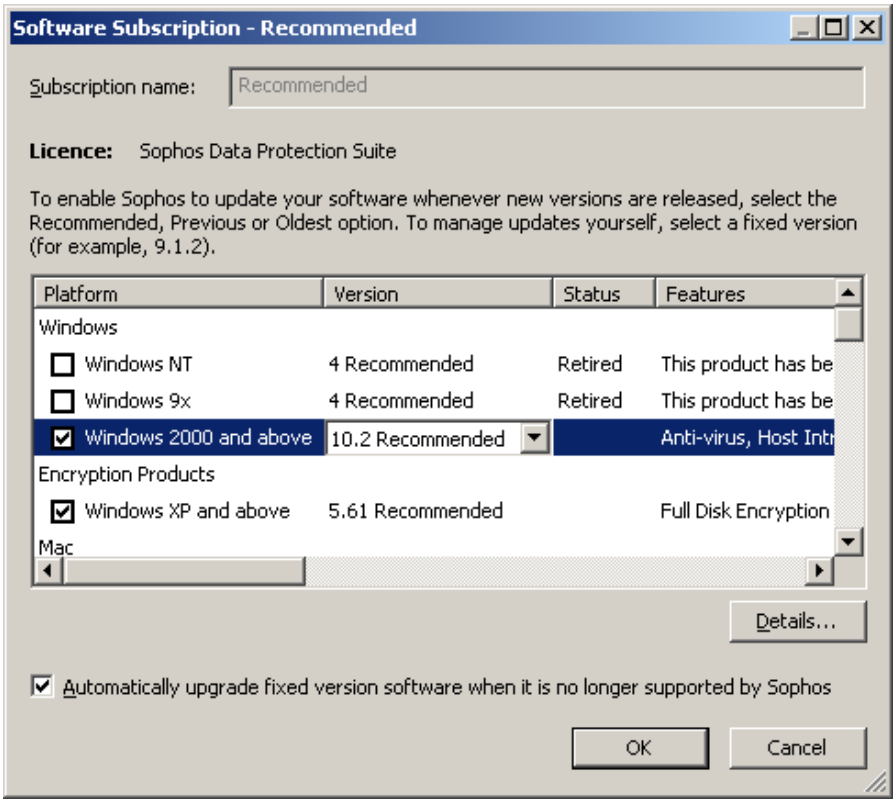


4.49. Clique com o botão direito do mouse no “Recommended” e clique em “View/Edit Subscription”.

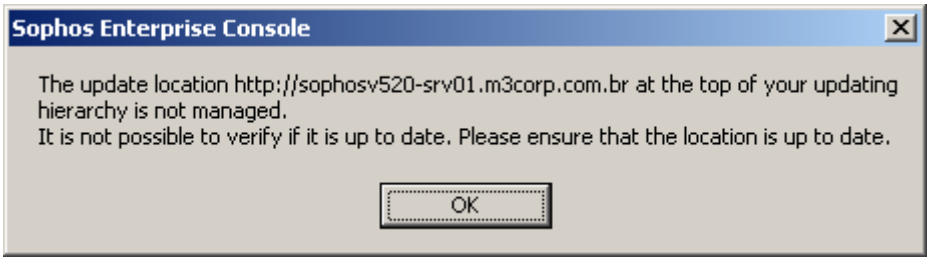


4.50. A janela “Software Subscription” irá abrir, na coluna “Platform” selecione as plataformas desejadas (onde o servidor do Sophos irá fazer o download dos arquivos de instalação para as plataformas selecionadas), clique no botão “OK”.

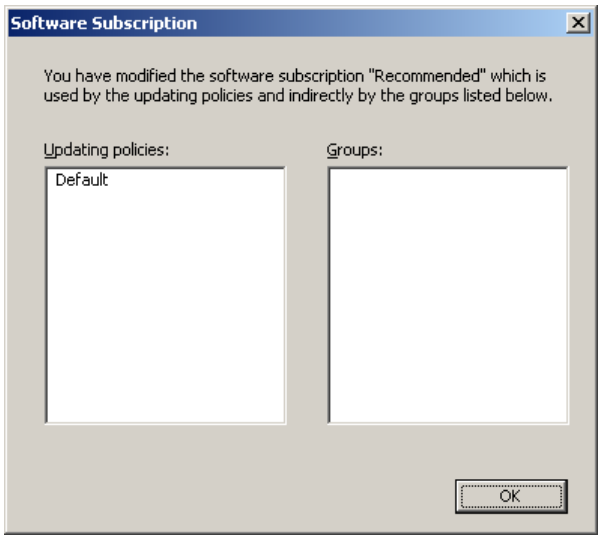
OBS: Caso queira, marque a opção “Windows XP and above” na categoria “Encryption Products” para usar a criptografia da Sophos.



4.51. Clique no botão “OK”.

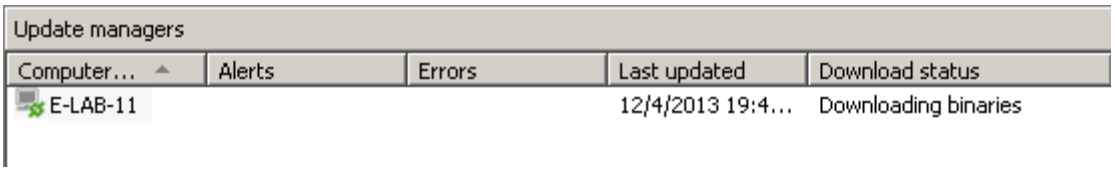

Sophos Enterprise Console
The update location http://sophosv520-srv01.m3corp.com.br at the top of your updating hierarchy is not managed.
It is not possible to verify if it is up to date. Please ensure that the location is up to date.
OK

4.52. Clique no botão “OK”.

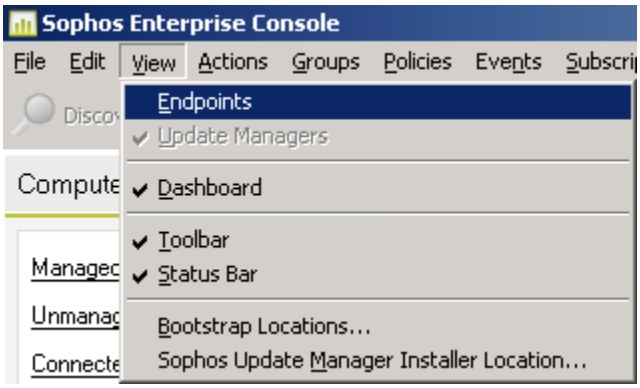

Software Subscription
You have modified the software subscription "Recommended" which is used by the updating policies and indirectly by the groups listed below.
Updating policies:
Default
Groups:
OK

4.53. A coluna “Download status” irá voltar a indicar “Downloading binaries”, o primeiro update (onde será realizado o download dos arquivos de instalação para cada plataforma selecionada anteriormente), quando o download finalizar, a coluna “Download status” irá indicar “Last checked at: <data>”, é necessário aguardar o download finalizar para:

- Fazer a instalação do Sophos Endpoint nas estações.
- Configurar algumas políticas como “Application Control” e “Data Control”, que dependem de algumas informações que são coletadas via update.



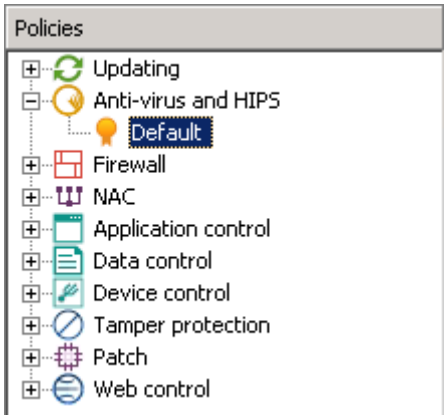
4.54. Para voltar a visualizar o painel dos “endpoints”, clique em “View” > “Endpoints”.



5. Configurações recomendadas

Neste item, será demonstrado às configurações recomendadas para novas implementações do Sophos, onde o foco é configurar o Sophos para não causar nenhum bloqueio indesejado, mantendo a proteção contra malwares. Após o período de implementação, é recomendado ativar os módulos do Sophos de forma gradual.

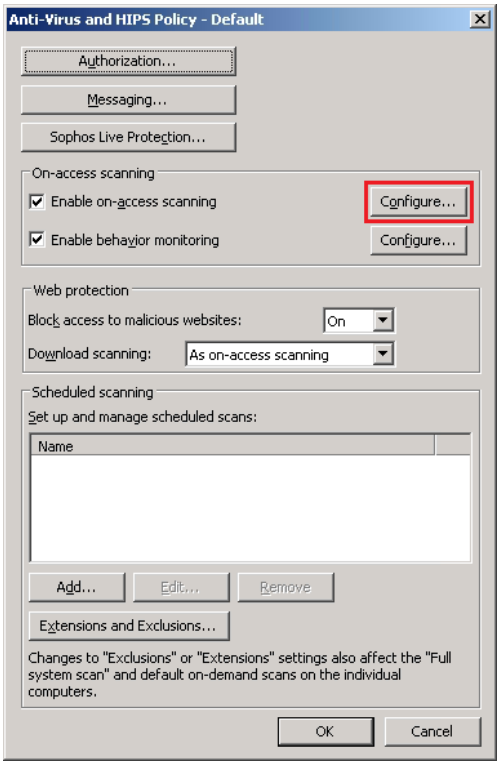
5.1. Anti-virus and HIPS



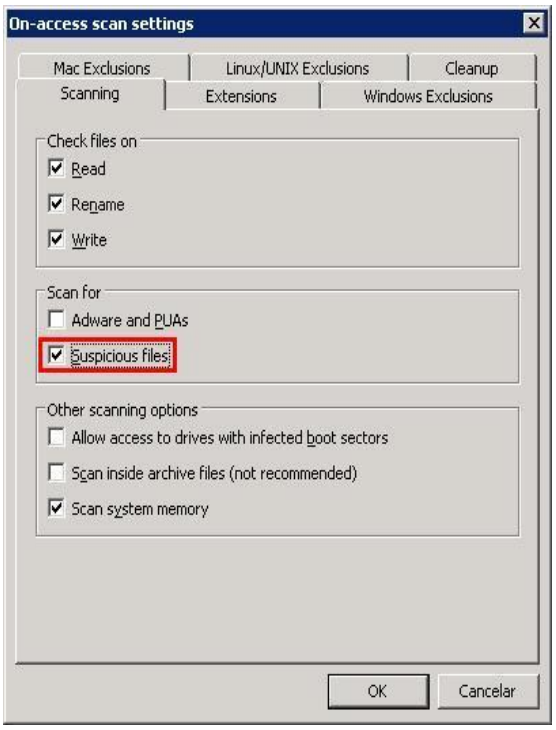
5.1.1. No Sophos Enterprise Console, expanda o item “Anti-virus and HIPS”.

5.1.2. Clique duas vezes na política de Antivírus e HIPS a ser editada (ou clique com o botão direito e clique em “View/Edit Policy”)

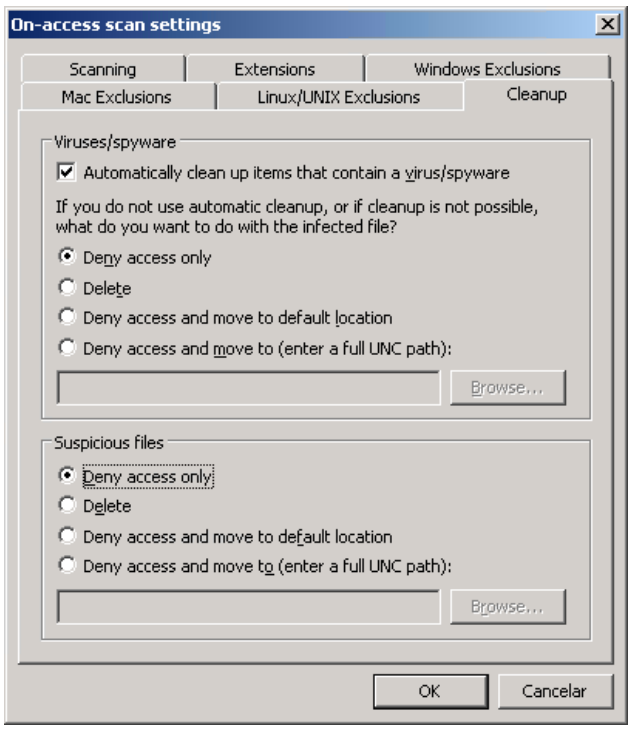
5.1.3. Em “Enable on-access scaning”, clique em “Configure...”.



5.1.4. Na guia/aba “Scanning” marque a opção “Suspicious files (HIPS)” para habilitar a analise por arquivos suspeitos.

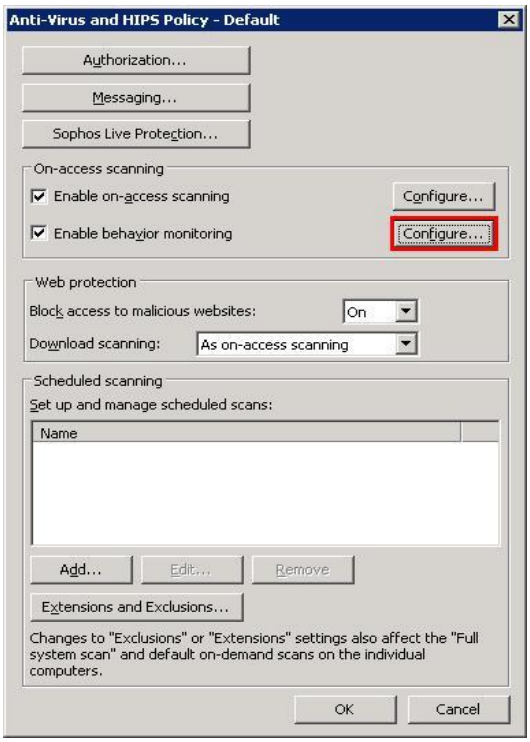


5.1.5. Na guia “Cleanup”, marque a opção “Automatically clean up item that contain a vírus/spyware”, e selecione as ações que devera ser usadas caso o cleanup não esteja disponível ou caso a opção de cleanup não esteja marcada, como o exemplo da imagem abaixo:

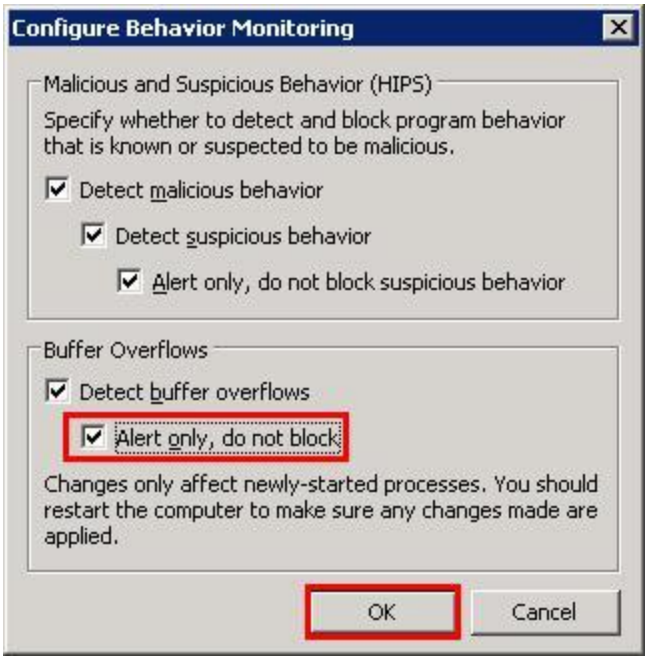

On-access scan settings
Scanning
Extensions
Windows Exclusions
Mac Exclusions
Linux/UNIX Exclusions
Cleanup
Viruses/spyware
Automatically clean up items that contain a virus/spyware
If you do not use automatic cleanup, or if cleanup is not possible, what do you want to do with the infected file?
Deny access only
Delete
Deny access and move to default location
Deny access and move to (enter a full UNC path):
Browse...
Suspicious files
Deny access only
Delete
Deny access and move to default location
Deny access and move to (enter a full UNC path):
Browse...
OK
Cancelar

5.1.6. Clique no botão “OK”.

5.1.7. Em “Enable behavior monitoring” clique em “configure...”

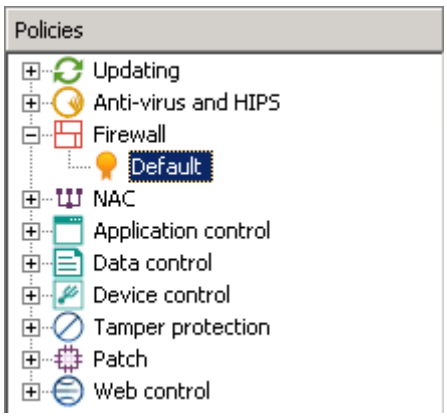


5.1.8. Em Buffer Overflows, habilite a opção “Alert only, do not block” e clique no botão “OK”.


Configure Behavior Monitoring
Malicious and Suspicious Behavior (HIPS)
Specify whether to detect and block program behavior that is known or suspected to be malicious.
Detect malicious behavior
Detect suspicious behavior
Alert only, do not block suspicious behavior
Buffer Overflows
Detect buffer overflows
Alert only, do not block
Changes only affect newly-started processes. You should restart the computer to make sure any changes made are applied.
OK
Cancel

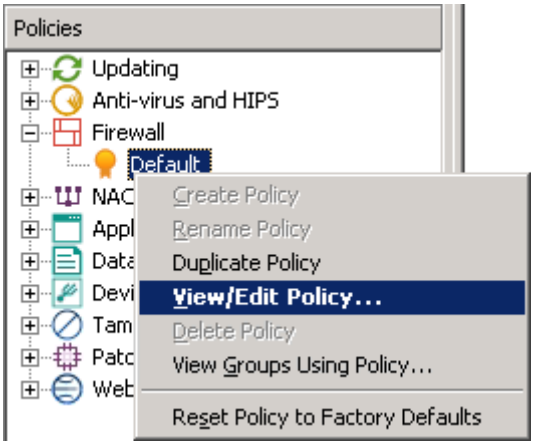
5.1.9. Aplique as alterações clicando no botão “OK”.

5.2. Firewall



5.2.1. No quadro “Policies”, expanda o item “Firewall”.

5.2.2. Clique com o botão direito na política “Default” (dentro o item “Firewall”) e clique em “View/Edit Policy”.



5.2.3. Na tela “Welcome to the firewall policy wizard”, clique em “Avançar”

5.2.4. Na tela “Configure firewall”, escolha a opção “Single location” e clique em “Avançar”

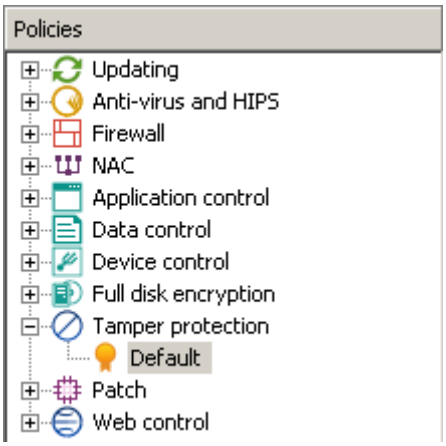
5.2.5. Na tela “Operational mode”, escolha a opção “Monitor” e clique em “Avançar”

5.2.6. Na tela “File and printer sharing”, escolha a opção “Allow file and printer sharing’ e clique em “Avançar”

5.2.7. Clique em “Concluir” para finalizar o assistente

5.3. Tamper protection

O Tamper protection impede que usuários não autorizados editem as políticas bem como desinstalar o Sophos Endpoint do computador, com isto, será necessário informar uma senha que foi previamente configurada nas políticas da console.



5.3.1. No quadro “Policies”, expanda o item “Tamper protection”.

5.3.2. Clique com o botão direito na política “Default” (dentro o item “Tamper protection”) e clique em “View/Edit Policy”.

5.3.3. Marque a opção “Enable tamper protection”.

5.3.4. Clique no botão “Set...”.

5.3.5. Em “Password”, informe a senha desejada.

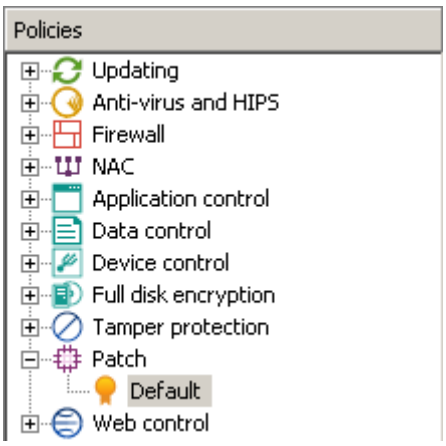
5.3.6. Em “Confirm password”, confirme a senha e clique no botão “OK”.

5.3.7. Clique no botão “OK”.

Tamper Protection Policy - Default
Enable tamper protection
Create or change the password that allows endpoint users to uninstall, disable, or re-configure Sophos Endpoint Security and Control.
Password:
Set...
OK
Cancel

5.4. Patch

Atualmente, 90% dos ataques podem ser evitados com um patch existente. No entanto, muitos computadores continuam em risco, pois identificar os computadores que estão sem um determinado patch pode ser uma tarefa difícil. Além de identificar os computadores que estão sem algum patch de correção, o Sophos Patch Assessment qualifica os patchs e identifica as ameaças que exploram a vulnerabilidade que o patch pode corrigir.



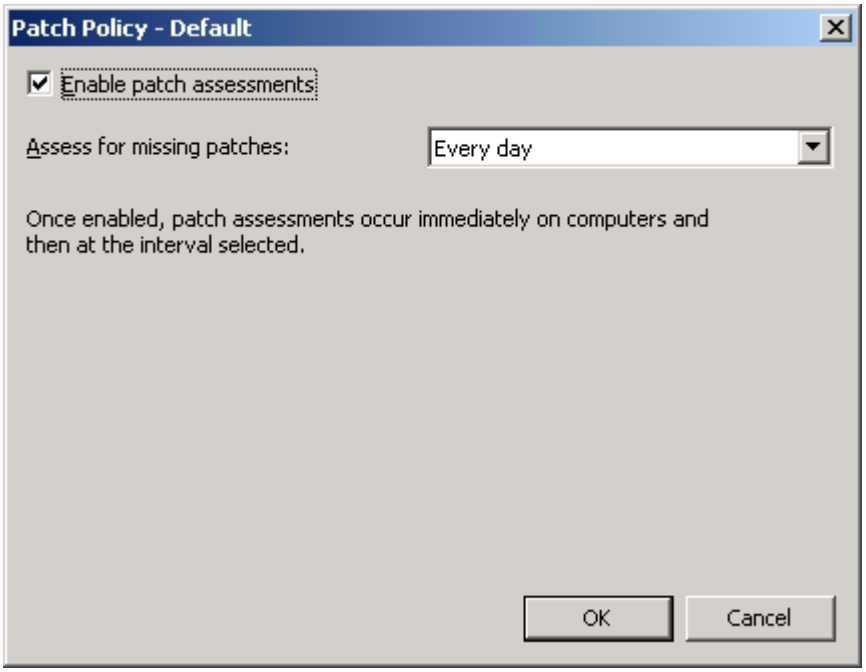
5.4.1. No quadro “Policies”, expanda o item “Path”.

5.4.2. Clique com o botão direito na política “Default” (dentro o item “Path”) e clique em “View/Edit Policy”.

5.4.3. Marque a opção “Enable patch assessments”.

5.4.4. Em “Assess for missing patchs”, selecione “Every day”.

5.4.5. Clique no botão “OK”


Patch Policy - Default
Enable patch assessments
Assess for missing patches:
Every day
Once enabled, patch assessments occur immediately on computers and then at the interval selected.
OK
Cancel

6. Instalando os endpoints (deploy)

Existem várias formas para realizar a instalação do software do endpoint, no entanto não é necessário realizar todas as opções. Para fazer o deploy, consulte o artigo AA-00218 em nossa base de conhecimentos, que descreve alguns métodos de deploy recomendados:

http://suporte.m3corp.com.br/article/AA-00218